programs which authenticate the user to RACF (or other host access control facility) to be modified to use the certificate instead of the traditional user ID (user identifier) and password. This requires an enterprise to upgrade each of its application subsystems in order to achieve the ~~benefits. So for some enterprises, the previous approach may be impractical and unacceptable,~~

U.S. 6823452

Related U. S. Patent 6823452 titled "Providing End-to-End User Authentication for Host Access Using Digital Certificates" and referred to hereinafter as "the related invention", discloses a technique for using digital certificates to authenticate a client in order to allow the client to access legacy host applications and/or data which are protected by a security system such as RACF, where these host applications or systems for managing host data (including legacy database systems) typically require a user identification and password that is supplied separate from that used for the client's sign-on process to the modern environment. Thus, the related invention enables the user to access a legacy host application and/or legacy host data with a single sign-on (i.e. without re-identifying himself), and does not require modifications to the legacy software.

In the related invention, SSL or a similar security protocol is used to establish a connection between a client device and either a Web application server or a Telnet 3270 ("TN3270") server. The client's digital certificate is required when establishing the SSL connection, according to the prior art SSL specification, to enable the Web application server or TN3270 server to authenticate the client. The certificate is then cached at the server, according to the related invention, and used to authenticate the client to the host-based, legacy security